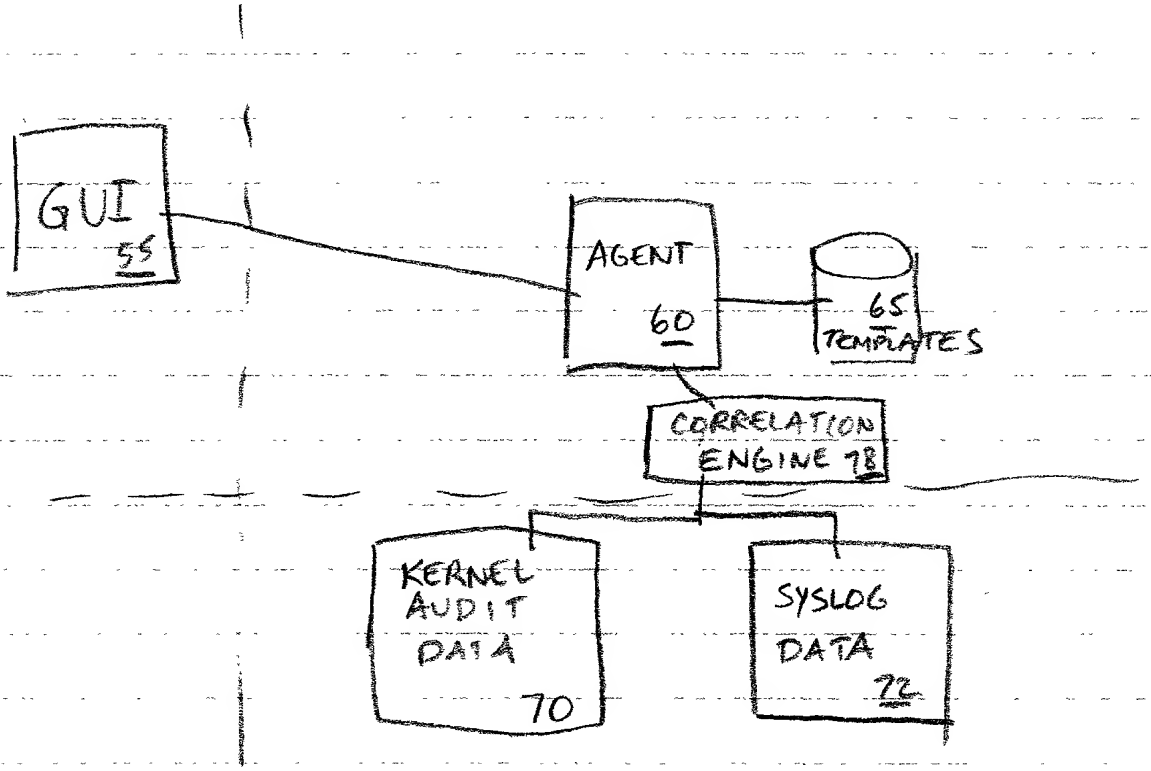
FIG.1


GUI
55
AGENT
60
65
TEMPLATES
CORRELATION
ENGINE 78
KERNEL
AUDIT
DATA
70
SYSLOG
DATA
72

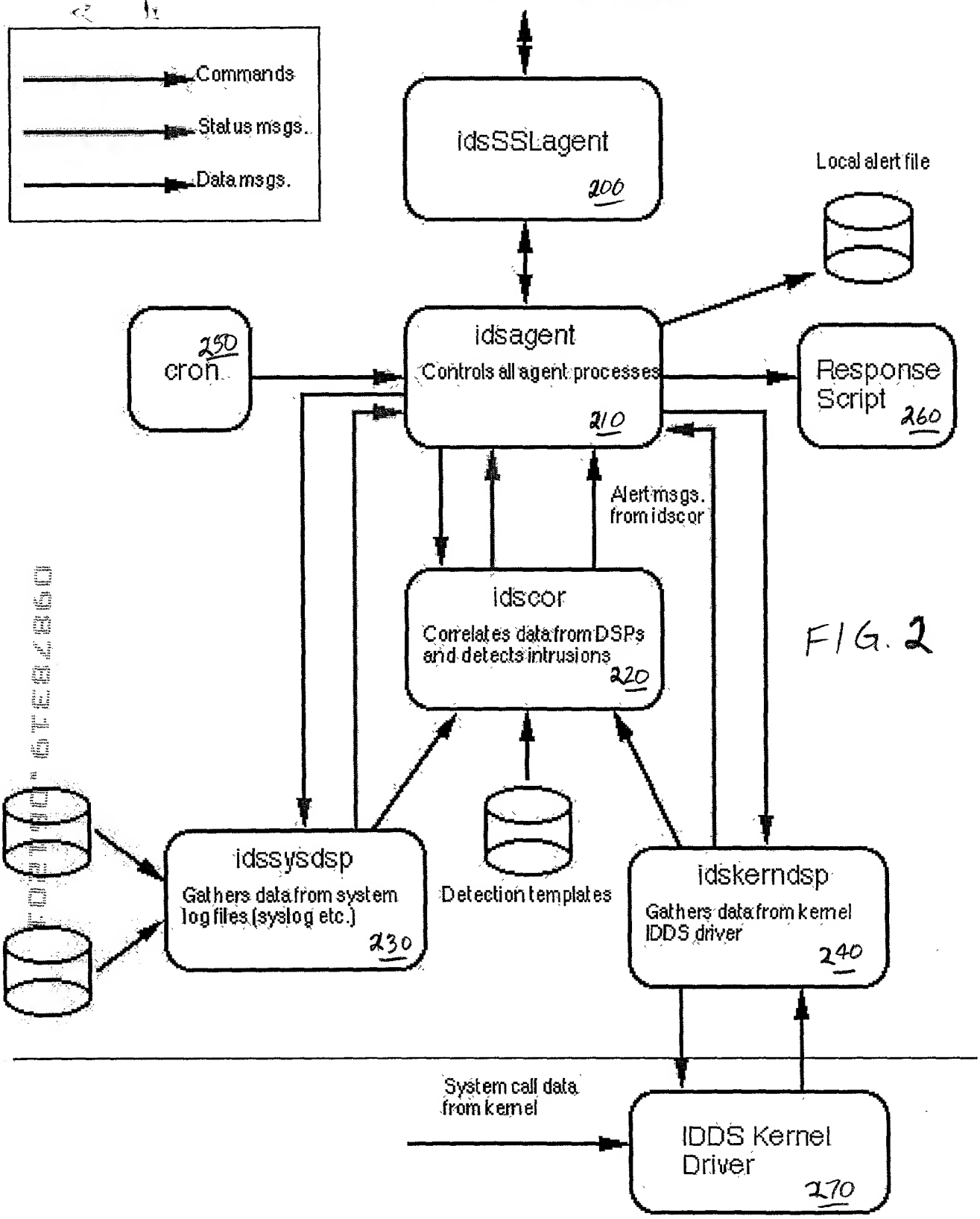

How do the agent processes fit together?
Commands
Status msgs.
Data msgs.
idsSSLagent
200
Local alert file
cron
250
idsagent
Controls all agent processes
210
Response Script
260
Alert msgs. from idscor
idscor
Correlates data from DSPs and detects intrusions
220
Operating System Audit Logs
idssysdsp
Gathers data from system log files (syslog etc.)
230
Detection templates
idskerndsp
Gathers data from kernel IDDS driver
240
System call data from kernel
IDDS Kernel Driver
270

FIG. 2

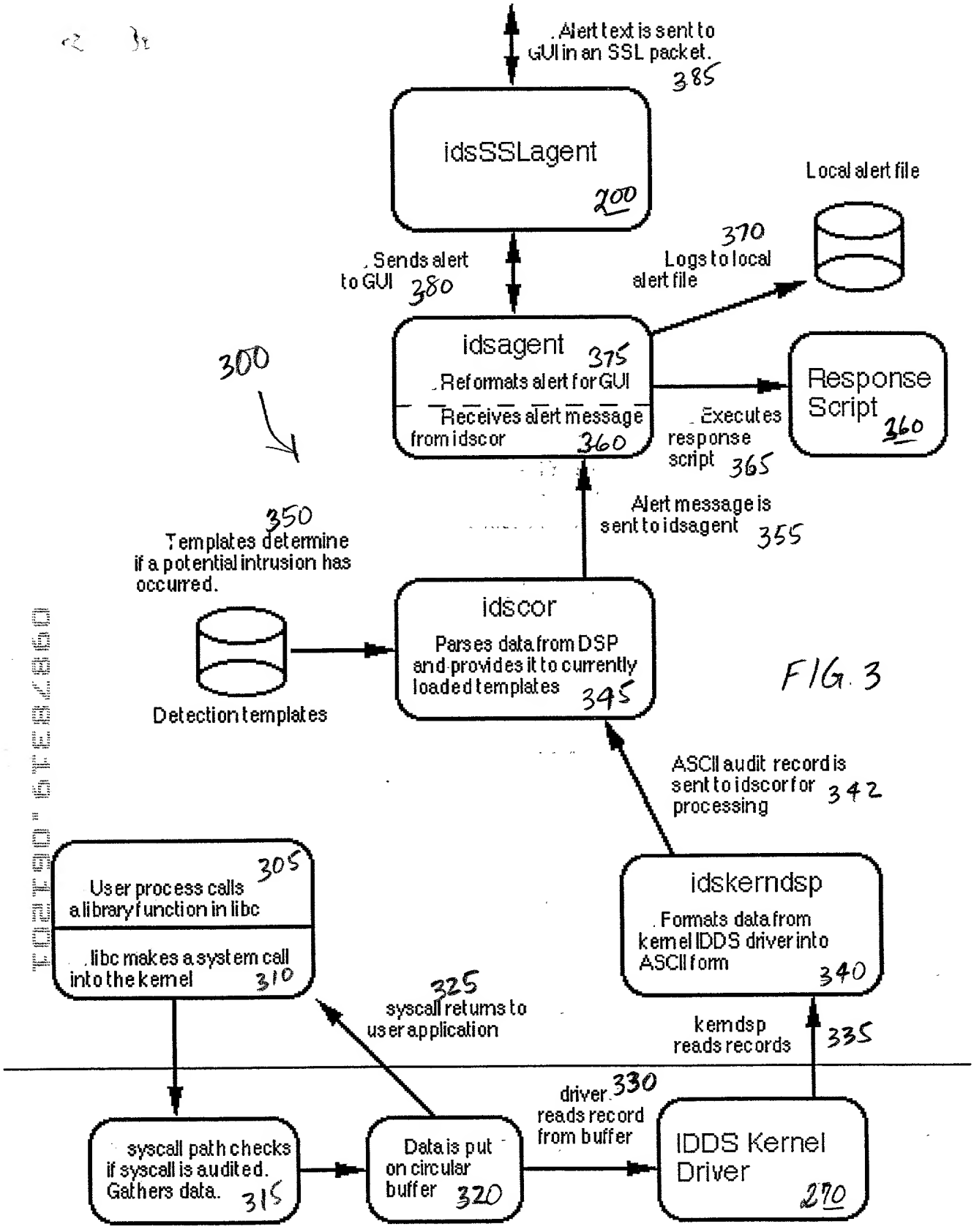

Alert text is sent to GUI in an SSL packet. 385
idsSSLagent 200
Local alert file
370 Logs to local alert file
Sends alert to GUI 380
idsagent 375
Reformats alert for GUI
Receives alert message from idscor 360
Response Script 360
Executes response script 365
300
Alert message is sent to idsagent 355
350 Templates determine if a potential intrusion has occurred.
idscor
Parses data from DSP and provides it to currently loaded templates 345
Detection templates
ASCII audit record is sent to idscor for processing 342
User process calls a library function in libc 305
libc makes a system call into the kernel 310
idskerndsp
Formats data from kernel IDDS driver into ASCII form 340
325 syscall returns to user application
kerndsp reads records 335
driver reads record from buffer 330
syscall path checks if syscall is audited. Gathers data. 315
Data is put on circular buffer 320
IDDS Kernel Driver 270

FIG. 3

FIG. 4

Infrastructure
- Agent Monitor
- Remote connection

Operation/Control
- Installation
- Initialization
- Configuration
- Control/Status

Correlator
- ECS engine core
- Circuit/data control modules
- Messaging control
- Status/Error/Trace output
- Command input and dispatch
- Engine state dump

Data Source Processes
- Audit
- Syslog
- Network

Detection Patterns
- Kernel patterns
- Network patterns(future)
- Web server patterns (from logs)

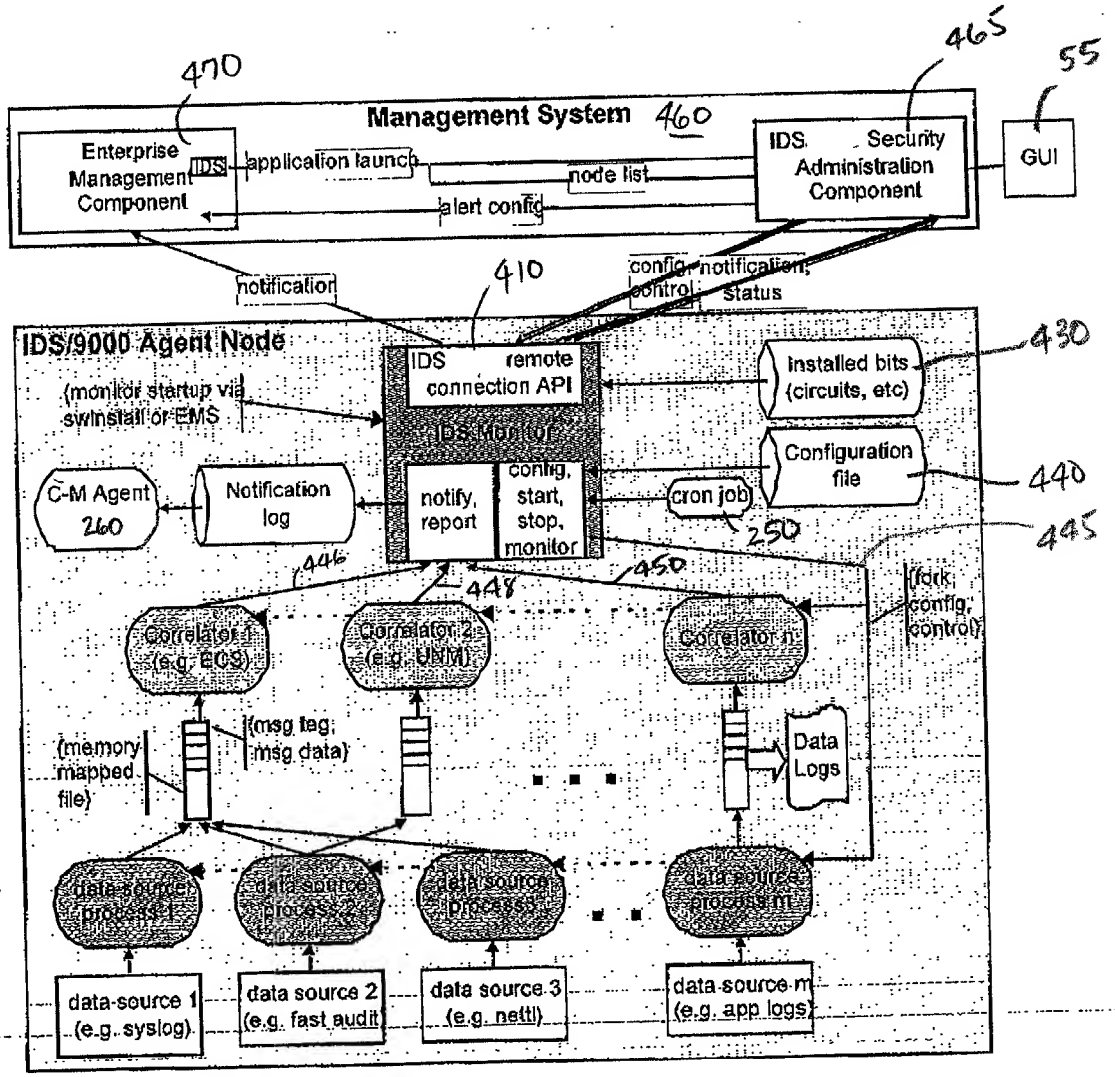


FIG. 5

Infrastructure

- Admin Core
- Remote connection
- Secure communications

Operation/Control

- Installation
- Initialization
- Configuration
- Control/Status
- Message handling
- GUIs